

Morrison & Foerster Client Alert.

February 5, 2013

FTC Announces Important Settlement with Social Networking App and Releases New Mobile App Report

By **D. Reed Freeman, Jr. and Nicholas Datlowe**

The FTC announced a potentially groundbreaking settlement with the social networking app Path and released an important new staff report on Mobile Privacy Disclosures¹ late last week.

The FTC's Settlement with Path suggests a new standard may be on the near-term horizon: out-of-policy, just-in-time notice and express consent for the collection of data that is not obvious to consumers in context. The FTC has long encouraged heightened notice and consent prior to the collection and use of sensitive data, such as health and financial information. This settlement, however, requires such notice and consent for the collection and use of information that is not inherently sensitive, but that, from the Commission's perspective, at least, might surprise consumers based on the context of the collection. Only time will tell, but historically Order provisions like this have tended to become cemented as FTC common law. Moreover, although the COPPA portions of the settlement do not break new ground, they do serve as a potent—and expensive—reminder that the FTC is highly focused on kids' privacy online, particularly in the mobile space.

The FTC's Report reinforces this sentiment by encouraging all the major players in the mobile ecosystem—including app developers, ad networks, and trade associations—to increase the transparency of the mobile ecosystem through clear, accessible disclosures about information collection and sharing at appropriate times.

THE PATH SETTLEMENT AND ORDER

The Path case touches on two areas that are now key parts of the FTC's enforcement program. This is the fifth COPPA case in the last two years, and

Beijing

Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels

Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong

Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London

Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles

Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York

Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia

Daniel P. Westman (703) 760-7795

Palo Alto

Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco

Roland E. Brandel (415) 268-7093
Anna Ferrari (415) 268-6728
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazacki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiko Terazawa 81 3 3214 6585

Washington, D.C.

Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

¹ As part of a flurry of activity, the FTC also released new online guidance for Mobile App Developers, and FTC Chairman Jon Leibowitz announced that he will step down on February 15, 2013.

Client Alert.

the second case involving mobile apps, all within the last eighteen months. The settlement reiterates the importance of living up to representations about privacy practices, and of making sure that your app, website, or online service takes action on any age-screening to avoid COPPA's notice and verifiable parental consent requirements.

According to the FTC, for about fifteen months between November 2010 and February 2012, Path's data collection practices on its mobile app violated Section 5 of the FTC Act, and its data collection practices for about eighteen months, ending in May 2012, violated the COPPA Rule. The FTC alleges that Path violated Section 5 by collecting data from users in a manner inconsistent with the representations in the app and in its privacy policy, and that it violated COPPA by knowingly collecting data from users under the age of 13 without verifiable parental consent.

Section 5 Violations

Path's social networking app allows users to create a simple journal (called a "path") of their lives and then to share that journal with a select group of people. According to the FTC, the app also enabled users to find friends to add to their network through a variety of means, including by searching contacts stored on the device. However, even when the user chose a different method of locating friends, the FTC alleged that Path *automatically and without user consent or knowledge* collected and stored personal information from the device's address book, including names, addresses, phone numbers, dates of birth, and more.

According to the FTC, Path's privacy policy also didn't give any indication that it was collecting this information. The app's privacy policy informed users that it collected only voluntarily given personal information, and automatically collected only information like IP address, operating system, and browser type. The privacy policy made no mention of the automatic collection and storage of information from the contacts in the user's address book. As the FTC stated in its Complaint, users "had no meaningful choice as to the collection and storage of personal information from [their] mobile device contacts." As a result, according to the FTC, the representations in the app privacy policy pertaining to the automatic collection of data, and the implication of the in-app choice that it would only collect personal information from the user's contact list if the user allowed it to do so were both false or misleading and constituted deceptive acts or practices in violation of Section 5 of the FTC Act.

COPPA Violations

Although the Path app invited users to provide their date of birth when they registered for the service, Path allegedly allowed users under the age of 13 to register and to use all of the features of the Path service, including sharing pictures, physical location, and other personal information. Path also automatically collected the same data from the contacts in children's address books that it collected from all other users, as discussed above.

COPPA and its implementing Rule require notice and verifiable parental consent before the collection, use, and/or disclosure of personal information collected from children online. Path allegedly violated COPPA by allowing children under the age of thirteen to use the app, by knowingly collecting personal information from them without clear notice, and by failing to provide parents with direct notice and obtain verifiable parental consent. In other words, Path collected age information, then allowed under-13 users to proceed, providing their personal information to the app. This was almost certainly a simple oversight, but it is the kind of basic blocking and tackling the FTC expects companies to get right. Path paid for its failure to do so with an \$800,000 civil penalty.

Client Alert.

THE CONSENT ORDER: PLAINTING A SEED FOR A NEW STANDARD?

As a result of its settlement with the FTC, Path is barred from engaging in the same type of allegedly deceptive and misleading practices regarding the collection and use of information; may not collect information from children in violation of COPPA; and must pay an \$800,000 civil penalty for the COPPA violations.

The Path Order may also signal a new shift by the FTC in its expectations of app developers and online companies generally. The Order requires the app to provide clear notice and obtain explicit consent before it may collect or access any information in a user's mobile device contacts or address book. Once the disclosure is made, before any such data can be collected, Path must "[o]btain the user's affirmative express consent to access or collect such information."

Even though this notice and consent requirement is ostensibly limited to Path, the Order sets a potential precedent for the regulation of the collection and usage of data in "non-obvious" or secondary situations. The FTC has emphasized the importance of heightened notice and express consent for these types of data collection, and in the just-released *Mobile Privacy Disclosures* Report (discussed in further detail below), the FTC recommends that apps provide "just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information." Here, however, the FTC has made it a legal requirement that Path do the same. Express consent under these circumstances would be a new requirement, and this case sets the FTC on that "path."

The FTC may consider this new express consent requirement of the Path Order "fencing-in relief," where because of previous acts leading to FTC enforcement action, respondents are forbidden by Order from engaging in certain practices that others may be allowed to engage in, in order to ensure that they do not approach the boundaries of acceptable behavior again. However, these fences may become everyone's fences. Just as, over time and through *ad hoc* enforcement, we have seen the FTC look for the disclosure of material facts in privacy policies, and then for the disclosure of such facts outside of privacy policies, it may be that the FTC will use the Path Order to begin to establish a new Section 5 expectation that the collection of non-obvious personal information, or the collection of information for secondary uses, which may be unexpected to users in context, *requires* additional notice and affirmative express consent to avoid Section 5 liability.

Path also must delete any information it improperly collected, and cease the collection going forward. Path is also enjoined from making misrepresentations relating to privacy of personal information, and must, as is now standard in FTC privacy orders, implement a comprehensive privacy program, engage a third party to perform privacy audits, submit compliance notices to the FTC for twenty years, and meet additional reporting and monitoring requirements.

THE FTC'S MOBILE PRIVACY DISCLOSURES REPORT

Along with the Path Order, FTC staff released a Report called *Mobile Privacy Disclosures: Building Trust Through Transparency*. The Report "offers several suggestions for the major participants in the mobile ecosystem as they work to improve mobile privacy disclosures." It focuses on enhanced disclosures to users regarding the collection and use of sensitive information, and continues a long line of efforts to issue Best Practices guidance, rather than merely using *ad hoc* Section 5 enforcement. This Report grew out of the "In Short" workshop on mobile advertising and privacy, held in May 2012.²

² This Report only deals with certain topics that were covered at the workshop. The FTC states that further guidance will emerge from that workshop, updating the "Dot Com Disclosures" that were first released approximately twelve years ago. This is the first time the FTC has confirmed that it will be releasing such guidance.

Client Alert.

For app developers, the Report's most important recommendation is that they "provide just-in-time disclosures and obtain affirmative express consent when collecting sensitive information outside the platform's API, such as financial, health, or children's data, or sharing sensitive data with third parties." Thus, even as app platforms deliver increasingly sophisticated disclosures to end-users, it remains incumbent on the developers themselves to ensure that their collection and use of important and sensitive personal information is clearly and appropriately disclosed. These disclosures cannot simply be repetitions of the general privacy policy disclosures, but rather should be specific to the data being collected and/or shared, and presented at the time the data are collected.

The Report also encourages developers to make a privacy policy readily available, to improve disclosures regarding data sharing with ad networks and other third parties, and to participate in self-regulatory programs and trade associations.

The recommendations for ad networks, other third parties, and trade associations are narrower. The Report primarily recommends improved coordination and communication so that, for instance, app developers know and understand what information advertising networks are collecting through their apps. Similarly, the Report recommends that ad networks coordinate with the platforms on the implementation of an effective do-not-track system for mobile. As for trade associations, the Report urges that they support educational efforts and work to promote uniform standards for privacy policies and disclosures. Such measures may include icons or badges that succinctly represent data collection, use, and sharing practices.

CONCLUSION

The Path Settlement provides another example of the FTC's expanding oversight and enforcement role with regard to privacy issues in the mobile ecosystem. Just as the new COPPA Rule that goes into effect in July expanded the definition of personally identifiable information to geolocation data and persistent identifiers such as IP addresses and unique device identifiers, this Order may mark the first step toward making enhanced notice and explicit affirmative consent legally binding requirements for the collection and use of personal information in non-obvious contexts.

The *Mobile Privacy Disclosures* Report further reinforces the FTC's concern with the collection and use of sensitive information and personal information in non-obvious contexts. In announcing the FTC Order on its blog, Path noted the technology developer's "tendency to focus all attention on the process of building amazing new things," and implicitly acknowledged the related tendency to overlook privacy-related requirements. Consistent with its emphasis on "privacy by design," the FTC is continuing to push all participants in the mobile app ecosystem to give privacy the same level of attention as innovation.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Client Alert.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: <http://www.mofo.com/privacy--data-security-services/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.